REMARKS

Claims 1-20 are pending in the present application. Applicants note that reference YZ-Putz has not been initialed by the Examiner on the PTO Form 1449, filed February 1, 2001. A copy of this form is enclosed. The Examiner is respectfully requested to initial this reference, sign and date the PTO Form 1149, and return it to Applicants' representative with the next Office Action. Reconsideration and allowance based on the following remarks are respectfully requested.

I. Objection to the Specification

The specification was objected to because the application, as filed, did not contain an Abstract of the Disclosure as required by 37 C.F.R. §1.72(b). In response, a copy of an Abstract of the Disclosure is submitted herewith on a separate sheet of paper.

II. Rejection of the Claims Under 35 U.S.C. §103(a)

Claims 1-20 were rejected under 35 U.S.C. §103(a) based on Raivisto (U.S. Pat. No. 6,081,601) in view of Lintulampi (WO 98/59513) and Luo (U.S. Pat. No. 5,909,491). The rejection is respectfully traversed since none of the cited references disclose, teach or suggest a method, a system, a network element or a mobile station wherein, *inter alia*, a second cipher key, configured to provide ciphering in a second network, is calculated either in the mobile station or in a first network when the mobile station operates in the first network (using a first cipher key). According to embodiments of the Applicants' invention, the second cipher key for the second network is already available when the mobile station is operating in the first network, e.g., before a potential handover situation.

A. Raivisto

In the Office Action, the Examiner conceded that Raivisto fails to teach calculating a second cipher key to be used for ciphering traffic between the mobile station and the second mobile communication network in the first mobile communication network when the mobile station operates in the first mobile communication network; transmitting information necessary for calculating the second cipher key from the first mobile communication network to the mobile station when the mobile station operates in the first mobile communication network; and calculating the second cipher key at the mobile station to be used for ciphering traffic between the mobile station and the second mobile communication network.

The Examiner contended, however, that the mediator (e.g. SMS-C) disclosed in Raivisto "provides calculation of the second key and transmittal of the encrypted message (with the second cipher key) to the second mobile (e.g. recipient)." Applicants respectfully disagree with the Examiner and submit that Raivisto fails to teach or suggest the feature of calculating a cipher key. Applicants note that Raivisto only discloses a method for arranging encryption in a wireless network, wherein a first encryption key is used for encrypting information between a first terminal and a network element ("mediator"), and a second encryption key is used for encrypting data between the mediator and a second terminal. (See col. 3, lines 23-49). In Raivisto, the mediator decrypts the message received from the first terminal and encrypts the decrypted message before sending it to the second terminal using the second encryption key. However, Raivisto is silent about arranging cipher key calculation in the mediator. Applicants point out that Raivisto merely states that the mediator receives a cipher key from a database (see col. 6, lines 6-9). Furthermore, Raivisto is silent about sending any information for calculation of a second cipher key to the mobile station.

B. Lintulampi

Lintulampi fails to overcome the deficiencies in Raivisto. Lintulampi discloses a method of operating a dual mode mobile telephone. Lintulampi also discloses that a handover may be made between GSM and UMTS networks based on the capability of a current network to serve the requested service. According to this method, roaming decisions are made based on service availability in candidate networks. In that regard, the Examiner's attention is directed to pages 6 and 7 in Lintulampi, where a description of handover procedure to a new network is provided. However, it is respectfully submitted that Lintulampi does not teach or suggest the feature of arranging calculation of a second cipher key in a first mobile communication network when the mobile station operates in the first mobile communication network and uses a first cipher key, or the feature of transmitting information necessary for calculating the second cipher key from the first mobile communication network to the mobile station, or the feature of calculating a second cipher key at the mobile station to be used for ciphering between the mobile station and the second network.. In particular, Lintulampi does not teach or suggest security arrangements in handover situations.

C. Luo

Luo fails to overcome the deficiencies in Raivisto and Lintulampi. Luo discloses a method for sending secure messages in telecommunication systems using public key

encryption. Luo merely discloses ordinary GSM encryption key generation procedures (which are also described in the present application on pages 1-4). According to these procedures, cipher keys are always generated in an authentication center, AuC, which is typically located as part of a home location register HLR. Therefore, for roaming mobile stations, the cipher key, Kc, is calculated in the same authentication center, AuC, and then transferred to a network element arranging the ciphering in the visited network. Applicants note that these procedures are disclosed in Luo in col. 2, lines 32-35. Thus, the cipher key, Kc, is calculated when the mobile station connects to the visited network and is then used in the visited network. With such a method, all traffic between the mobile station and the visited network is transferred unciphered before the cipher key, Kc, is arranged in the mobile station and in the visited network. However, Luo does not disclose, teach or suggest cipher key generation according to the present invention. In particular, it is respectfully submitted that Luo does not disclose, teach or suggest, *inter alia*, the features of calculating a second cipher key in a first mobile communication network when the mobile station operates in the first mobile communication network and uses a first cipher key; transmitting information necessary for calculating the second cipher key from the first mobile communication network to the mobile station; or calculating the second cipher key at the mobile station to be used for ciphering between the mobile station and the second network.

For at least the above reasons, the cited references clearly fail to teach or suggest all of the features recited in claim 1. Therefore, even assuming that it would have been obvious to combine the cited references, which Applicants do not concede, the combination of Raivisto, Lintulampi and Luo would not have resulted in the invention of claim 1. Claims 2-11 are patentable by virtue of their dependency from claim 1 and for the additional features recited therein.

Claim 12 is patentable over Raivisto, Lintulampi, Luo or a combination thereof for at least the same reasons set forth above related to claim 1. Dependent claims 13-18 are patentable by virtue of their dependency from claim 12 and for the additional features recited therein. Similarly, claims 19 and 20 are patentable over Raivisto, Lintulampi, Luo or a combination thereof for at least the same reasons set forth above related to claim 1.

Accordingly, reconsideration and withdrawal of the rejection of claims 1-20 under 35 U.S.C. §103(a) based on Raivisto in view of Lintulampi and Luo are respectfully requested.

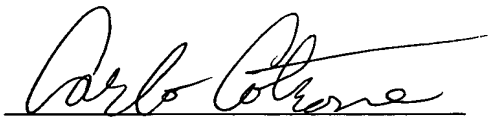
III. Conclusion

All rejections and objections have been addressed. It is respectfully submitted that the present application is now in condition for allowance, and a notice to that effect is earnestly solicited. Should there be any questions or concerns regarding this application, the Examiner is invited to contact the undersigned at the below-listed telephone number.

Please charge any fees associated with the submission of this paper to Deposit Account Number 033975. The Commissioner for Patents is also authorized to credit any over payments to the above-referenced Deposit Account.

Respectfully submitted,

PILLSBURY WINTHROP LLP

By: 

CARLO M. COTRONE
Reg. No. 48715
Tel. No. (703) 905-2041
Fax No. (703)-905-2500

CMC/CFL
Date: May 26, 2004
P.O. Box 10500
McLean, VA 22102
(703) 905-2000

ABSTRACT OF THE DISCLOSURE

A method of arranging data protection in a telecommunication system including a first mobile communication network, a second mobile communication network, and a mobile station supporting both of the mobile communication networks is disclosed. The method includes ciphering traffic between the mobile station and the first mobile communication network using a first cipher key; calculating a second cipher key to be used for ciphering traffic between the mobile station and the second mobile communication network in the first mobile communication network when the mobile station operates in the first mobile communication network; transmitting information necessary for calculating the second cipher key from the first mobile communication network to the mobile station when the mobile station operates in the first mobile communication network; and calculating the second cipher key at the mobile station to be used for ciphering traffic between the mobile station and the second mobile communication network.